PIERCE COUNTY
HAZARD IDENTIFICATION AND RISK ASSESSMENT

CYBER ATTACK[1]

Table of Contents

Identification and Description

Definition

"An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."[2] These attacks are efforts to exploit targeted systems for personal, political, social or financial reasons.

Types

Cyber-attacks are methods of action used within the greater context of the political, social and criminal realms. They are conducted by actors under the general context of:

- Cyber Warfare: Politically motivated actions by a nation-state to penetrate another nation's computers or networks for the purpose of conducting espionage or causing damage or disruption of national systems.[3]
- Cyber Terrorism: The intentional use of computers, networks and public internet to cause destruction and harm for personal objectives. These objectives may be political or ideological.[4]
- Cyber Crime: A crime which a computer is the object of the crime (hacking, phishing, spamming, ransomware) or is used as a tool to commit an offense (child pornography, hate crimes, theft, stalking…).[5]

Profile

Location and Extent

In 2009, President Obama stated in a speech about cyber security "…it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation."[6] Cyber-attacks can come in different forms based on the intended outcome and what is being attacked. Therefore, it is very difficult to define the specific methods, extent of the risk or target location. Any computer, computer system or electronic communications device/network is potentially vulnerable.

Attack methods are evolving and changing at an ever-increasing pace as technology changes and security efforts become steadily more advanced. For the purpose of this risk assessment, attack methods fall into the following general categories:

- Penetration Attack. This involves breaking into a system using a known security vulnerability to gain access.[7] Once access is gained the attacker can take control of the system, disrupt its functionality, incapacitate it, steal/gather information, conduct surveillance etc. These attacks can be very surreptitious and go undetected for extended periods, leaving the attacker ample time and opportunity to carry out their activities.

- Denial of Service Attacks. These affect a system by diminishing its ability to function and can eventually result in the incapacitation of that system.[8] The basic tactic is to overload the system's capability by flooding it with information such as e-mails, web site hits, significant increase in data streams etc.

Attacks can be designed to hit a specific target or accomplish a specific task then self-destruct. Others may be designed to gain access then "hide and report". Some can be designed like a time bomb that activate at a certain point or when specific criteria are met. Others are designed to spread as quickly and as far as possible to create the greatest impact or affect. Just as a human contagion can spread with every contact between people, an electronic contagion can spread at every point there is contact between an infected computer and any other electronic system capable of processing information. It then grows exponentially over time creating greater potential for long term impacts. The most important concept to be understood is that anything connected to or controlled by a computer that is capable of establishing contact with another computer or system is vulnerable to attack and exploitation.[9]

Occurrences

No specific data was found listing occurrences of cyber-attacks specific to Pierce County or Western Washington. The below table captures many reported incidents in the United States between late 2010 and early 2013.[10] Given the nature of the cyber environment, this list can be very representative of incidents that likely have and certainly will occur in the future in Pierce County.

Table CA-1 Reported Incidents in the United States Between Late 2010 and Early 2013

Date	Incident
October 2010	The Wall Street Journal reports that hackers employed malware programs to steal over $12 million from five banks in the US and UK.
March-April 2011	The FBI identified twenty incidents where online banking credentials of small-to-medium US companies were stolen and used to transfer over $11 million into Chinese companies.
March-April 2011	Hackers attempted to steal authentication data that would allow them to access the Lockheed Martin data networks.
April 2011	Google reported attempts to hack into their systems to compromise Gmail account passwords for prominent US people, to include senior US officials.
April 2011	Oak Ridge Laboratory employees received e-mails with malware attachments that infected two machines and resulted in a few megabytes of data being stolen. This was the second intrusion into the lab's data files.
May 2011	Hackers attacked Sony's PlayStation network and stole more than 80 million users' personal information. The loss was estimated at over $170 million.
June 2011	Citibank reported losing credit card data for 360,000 customers due to hacker activity.
July 2011	The Secretary of Defense announced that a defense contractor was hacked and lost 24,000 files.
September 2011	A malware program was introduced onto control stations for US Air Force Unmanned Arial Vehicles at Creech Air Force Base in Nevada. No drones were compromised, but the capability to remotely access UAV control systems was made clear.
October 2011	The networks for 48 chemical, defense and other industries were penetrated for at least six weeks by a hacker looking for intellectual property.

December 2011	US Chamber of Commerce announced that its computer networks were penetrated by a foreign hacker for nearly a year. The hacker had access to significant amounts of information, to include member company communications and industry positions on US trade policy.
March 2012	NASA's Inspector General reported that successful attacks on NASA computer systems resulted in the loss of 150 user credentials, which could be used to gain unauthorized access to NASA systems.
March 2012	DHS issued a cyber intrusion warning alert regarding attempts to infiltrate US gas pipeline systems.
June 2012	A phishing campaign targets US aerospace industry experts attending the 2013 IEEE Aerospace Conference.
July 2012	The Director of the NSA reported a 17-fold increase in cyber incidents at US infrastructure companies between 2009 and 2011.
December 2012	Two power plants hit with sophisticated malware infections gave attackers access to plant computer systems.
February 2013	The Department of Energy confirmed that it was hit by a major cyber-attack. Fourteen servers and 20 work stations were penetrated, which compromised the personal information of several hundred employees. The DOE is assuming that the attack was intended to obtain more sensitive information.
February 2013	DHS issued a restricted report revealing that criminals targeted 23 gas pipeline companies and stole information that could be used to commit sabotage.

In addition to this list, the DHS reported that there was a spike in 2012 of cyber-attacks against power, water and nuclear targets within the US. Gas pipeline and chemical companies were frequent targets as well. In some of the attacks, companies reported that some of the data which was stolen could allow for unauthorized remote operations of company systems.[11]

Recurrence Rate

Cyber incidents are expected to be a problem for the foreseeable future and recurrences are very likely to occur throughout Pierce County.

Impacts

Health and Safety of Persons in the Affected Area at the Time of the Incident

Cyber-attacks can be used to target specific individuals. Others, although not targeted at a specific person, seek to obtain information that can be used to harm people. Cyber bullying, stalking, identity theft, fraud, compromise of personal information or some other types of attacks, are all forms of cyber-crimes that affect people directly. These attacks frequently have significant psychological impacts, can dramatically impact on a person's well-being and have led to suicide in some cases.

Some denial of services attacks seeks to overload emergency communications systems. When successful, they can effectively shut down a community's 911 center leaving people without ready access to emergency services. If an attack of this nature were to occur in conjunction with another emergency, the potential for loss of life increases dramatically.

Some medical devices are drawing concern in recent media releases, because they broadcast information wirelessly to other medical systems. This makes them vulnerable to interdiction by a hacker. Recent advances in pace makers have included the ability to transmit data about a patient's heart directly to his or her doctor. Some are growing concerned that this may allow hackers to seize control over the device and disrupt its life saving function.[12] No further information was found to indicate that such an attack had taken place, however the potential exists.

Researchers at the University of Washington and University of San Diego demonstrated the ability to hack into a car's computerized systems and gain control over them, ignoring driver input.[13] Functional systems such as stability control, traction control, breaking, navigation systems, anti-theft systems, monitoring systems etc., are essentially wireless computer systems on many high-end cars that can communicate with each other as well as external systems such as OnStar, a smart phone or personal e-mail system. This makes them vulnerable to intrusion and incapacitation.[14] An attack on these systems poses significant risks to motorists for serious accident, injury and potentially death.

Successful attacks on critical infrastructure such as ground traffic control devices, railroad switches and air traffic control systems can result in catastrophic accidents with significant loss of life. Water management systems at some of the state's largest dams are controlled by networked computers. If remotely accessed, it is possible that a hacker could open the flood gates and release massive amounts of water onto downstream communities with disastrous effects.

This list could continue. The bottom line is that people have become inextricably linked to technological systems. While this link can benefit them in many ways, it also makes them vulnerable.

Health and Safety of Personnel Responding to the Incident

Emergency responders are most at risk if there were a successful attack on their supporting communications systems. Most radio and dispatch systems today are essentially computer networks. Disruption of that network poses great risk to responders as well as the public.

Continuity of Operations and Delivery of Service

Most county agencies rely very heavily on computer networks to function. Pay systems, personnel systems, social services, public works, judicial, emergency management etc., all require significant automated capability to function in modern society. Disruption of those systems will cause at least a short-term impact on a department's ability to operate, unless there are back-up protocols in place. Destruction of systems will likely extend the period in which operations are reduced or suspended.

Depending on what type of service an organization provides, delivery may be partially or completely disrupted. Agencies may be forced to temporarily suspend services until an attack can be stopped and systems restored. If the attack erases essential information, it may be a long period of time before an agency can return to normal levels of service delivery.

Property, Facilities and Infrastructure

There is significant potential for damage to facilities and infrastructure. Power generation and management systems, water movement and storage, waste water treatment facilities and gas pipelines are all controlled by computerized systems. A successful attack to gain control over these systems could result in extensive damage that may seriously reduce their capability for a period of time. Several incidents of damaging cyber-attacks on infrastructure have been reported throughout the world.[15] The potential for such an incident occurring in Pierce County is high.

Incapacitated transportation management and control systems could result in accidents that can severely damage property and facilities as well as creating potentially serious hazardous material threats.

The Environment

As previously mentioned, hazardous materials spills are a real possibility if automated protection systems are taken over and incapacitated. Failed transportation control systems may result in fuel spills as well as other hazardous cargo. Waste water treatment facilities could be temporarily disabled leaving large amounts of untreated sewage to potentially flow into local bodies of water.

Economic and Financial Condition

Most notable cyber-attacks resulted in significant financial impacts. System outages, lost customer information, stolen funds, stolen intellectual information etc., have frequently cost companies of all sizes large amounts of money. In 2012, the Ponemon Institute completed a three-year study in which it tracked 56 large US corporate organizations. The study showed an average annual financial loss of $8.9 million, with the largest loss being $46 million. The study further noted that smaller organizations incurred a significantly higher per capita cost, presumably the result of a less robust financial margin.[16]

Companies can incur substantial costs in their efforts to protect themselves from cyber-attack. Studies have shown that the stronger the security posture, the lower the costs associated with an attack.[17] These protective protocols and systems cost businesses money, which eventually is passed on to the client or consumer. Either way, the “threat” of cyber-attack is costing everyone more money.

Identity theft costs people significant amounts of money each year as bank accounts are drained, credit cards are fraudulently used, or personal information is used to make fraudulent transactions. In 2010, 8.1 million Americans were reportedly victims of identity theft with a mean loss of $631.00 per victim.[18] This equates to an annual consumer loss of over $5 billion.

Loss of customer information frequently equates to loss of confidence and ultimately loss of business. Larger companies are postured to survive this type of event. Small business, however, may lack the financial resources to rebound after such an incident.

The recovery costs could be extensive as well. Whether it is infrastructure damage, loss of funds, costs associated with correcting problems or loss of productivity, there may be a significant cost associated with putting things back together after a successful attack. Loss of information poses one of the greatest risks as its effects have the potential to linger well after the attack has been contained.

Public Confidence in the Jurisdiction's Governance

Cyber-attacks against the private sector will likely not impact on the public's confidence in their elected leaders, unless the targets of the attacks are of public interest such as a privately-owned utility or privately contracted public service. The greater the public impact, the greater potential that residents will question what their government is doing for them.

A loss of private information by a government agency has significant potential to impact public confidence. Residents expect that their private information will be protected. Just as a business, customer confidence drops if that information is compromised.

A sustained loss or reduction in a government provided service as a result of cyber-attack may erode public confidence. Generally speaking, the average citizen understands that things can happen. How quickly the agency recovers and returns to normal operations may directly impact on the level of confidence affected resident have. Over time, unaffected residents may begin to question the vulnerability of other agencies or systems, especially any system that contains their personal information.

Resource Directory

Regional

- **Homeland Security Region 5 Cyber Concept of Operations**
  Due to the sensitive nature of this plan it is only available by request through Pierce County Emergency Management.
- **Pierce County Prosecuting Attorney's Office- ID Theft/Cybercrime**
  http://www.co.pierce.wa.us/index.aspx?ind=2037
- **Pierce County Department of Information Technology**
  http://www.co.pierce.wa.us/Index.aspx?NID=111

National

- **Department of Homeland Security Critical Infrastructure Resource Center**
  http://training.fema.gov/EMIWeb/IS/IS860a/CIRC/infoTech1.htm
- **FEMA IT Disaster Recovery Plan**
  http://www.ready.gov/business/implementation/IT
- **Congressional Research Service- Identity Theft: Trends and Issues**
  http://www.fas.org/sgp/crs/misc/R40599.pdf
- **National Emergency Number Association- Best Practices Checklist for Denial of Service Attacks Against 9-1-1 Centers**
  http://www.nena.org/news/120618/Best-Practices-Checklist-for-Denial-of-Service-Attacks-Against-9-1-1-Centers.htm
- **Federal Bureau of Investigation Internet Crime Compliant Center**
  https://www.ic3.gov/default.aspx
- **Cyber Security & Information Systems Information Analysis Center**
  https://www.thecsiac.com/#section=most_viewed_content

Endnotes

[1] This assessment was reviewed by the Pierce County Regional Intelligence Analyst under the Washington State Fusion Center November 2019.

[2] Computer Security Resource Center. National Institute of Standards and Technology. Accessed April 28, 2020 from https://csrc.nist.gov/glossary/term/Cyber_Attack

[3] Taylor, R. W., Fritsch, E. J., Liederbach, J., & Holt, T. J. (2011). *Digital crime and digital terrorism* (2nd ed.). Upper Saddle River, NJ, New Jersey: Prentice Hall.

[4] Ibid.

[5] Federal Bureau of Investigation. "What We Investigate, Cyber Crime". Accessed April 28, 2020 from https://www.fbi.gov/investigate/cyber

[6] President Barak Obama speech on "Securing Our Nation's Cyber Infrastructure", March 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

[7] Dr. Joseph M. Kizza, University of Tennessee at Chattanooga, PowerPoint presentation- "Chapter 3: Types of Cyber Attacks", www.utc.edu/~jkizza/Books/CyberEthics/CyberNotes/Chapter3.ppt

[8] Ibid.

[9] Department of Homeland Security, Industrial Control Systems- Cyber Emergency Response Team, "Overview of Cyber Vulnerabilities", http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

[10] James Andrew Lewis, Center for Strategic and International Studies, Significant Cyber Incidents Since 2006, March 18, 2013, http://csis.org/files/ublications/1303189_significant_syber_incidents_since_2006.pdf

[11] David Goleman, CNNMoney, Hacker Hits on U.S. Power and Nuclear Targets Spiked in 2012, http://money.cnn/com/2013/01/09/technology/security/infrastructure-cyber-attacks/index

[12] Sharon Weinberger, AOL News, Five New Frightening Types of Cyberattacks, http://www.aolnews.com/2010/10/18/five-new-frightening-types -of-cyberattacks/

[13] Ibid.

[14] Dennis K. Nilsson and Ulf E. Larson, A Roadmap for Securing Vehicles Against Cyber Attacks, http://varma.ece.cmu.edu/Auto-CPS/Nilsson_Chalmers.pdf

[15] James Andrew Lewis.

[16] Ponemon Institute, 2012 Cost of Cyber Crime Study: United States, October 2012, page 3, http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

[17] Ponemon Institute, page 4.

[18] Kristin M. Finklea, Congressional Research Service, Identity Theft: Trends and Issues, February 15, 2012, page 1, http://www.fas.org/sgp/crs/misc/R40599.pdf